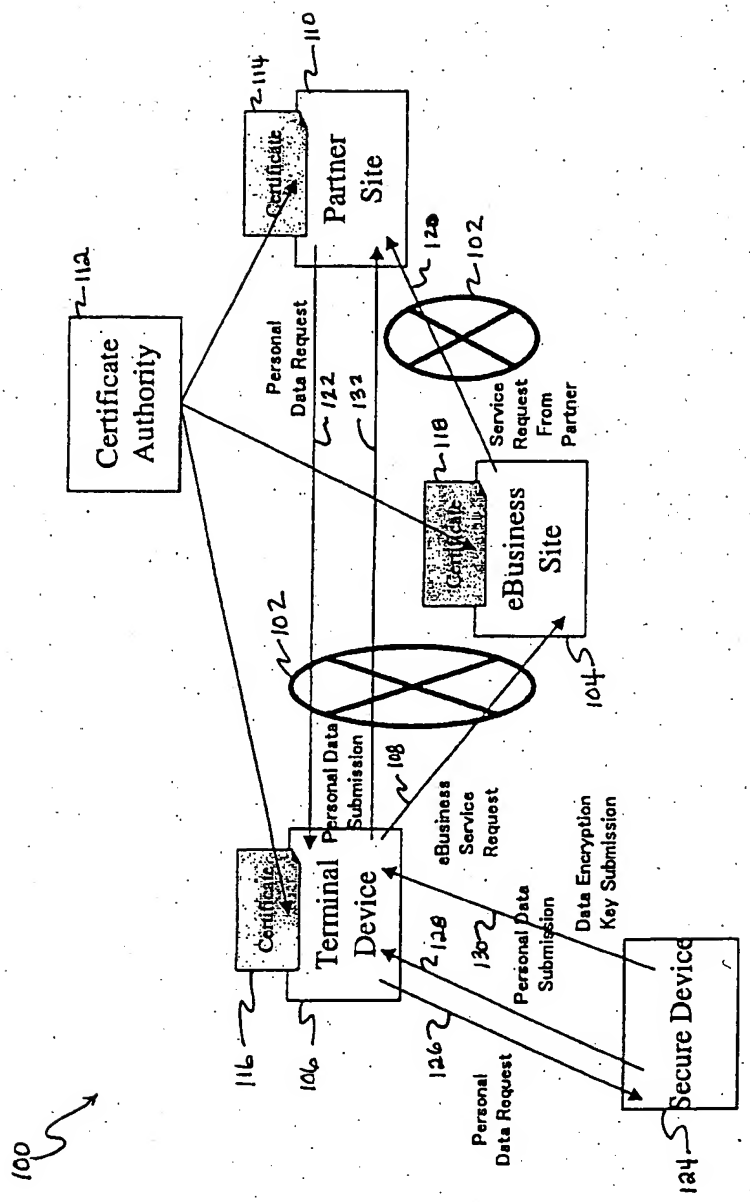
100
Certificate Authority
112
Certificate
114
Partner Site
110
120
102
Personal Data Request
122
132
Service Request From Partner
Certificate
118
eBusiness Site
104
102
Personal Data Submission
108
eBusiness Service Request
Certificate
116
Terminal Device
106
128
130
126
Personal Data Request
Personal Data Submission
Data Encryption Key Submission
Secure Device
124

FIG. 1

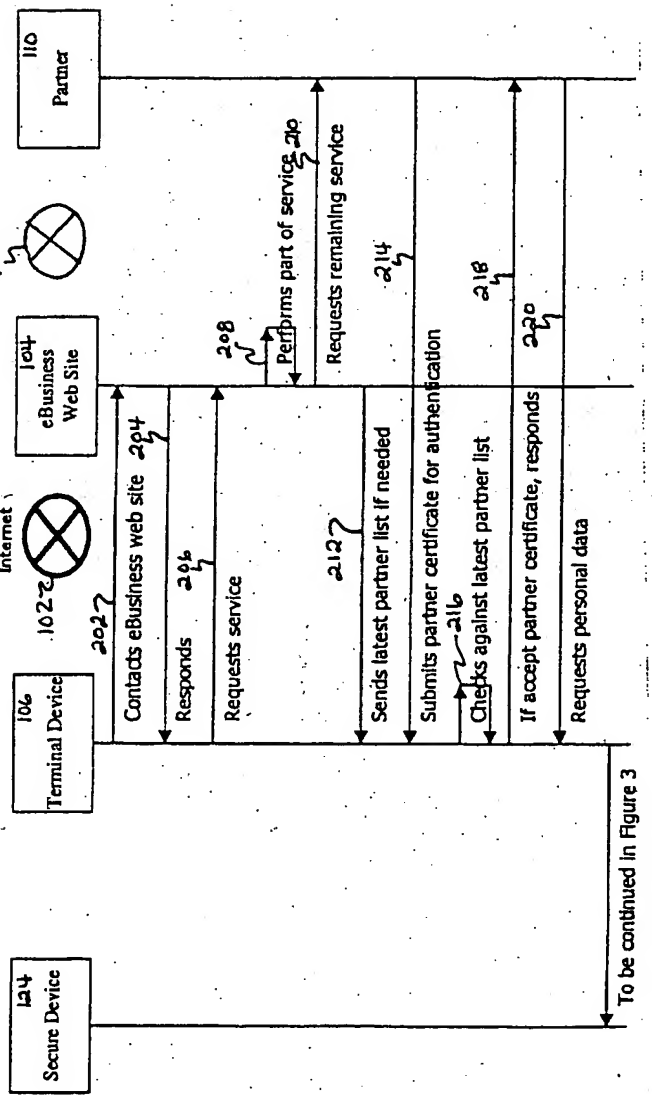
110
Partner
102
104
eBusiness Web Site
Internet
102
106
Terminal Device
124
Secure Device
202
Contacts eBusiness web site
204
Responds
206
Requests service
208
Performs part of service
210
Requests remaining service
212
Sends latest partner list if needed
214
Submits partner certificate for authentication
216
Checks against latest partner list
218
If accept partner certificate, responds
220
Requests personal data
To be continued in Figure 3

FIG. 2

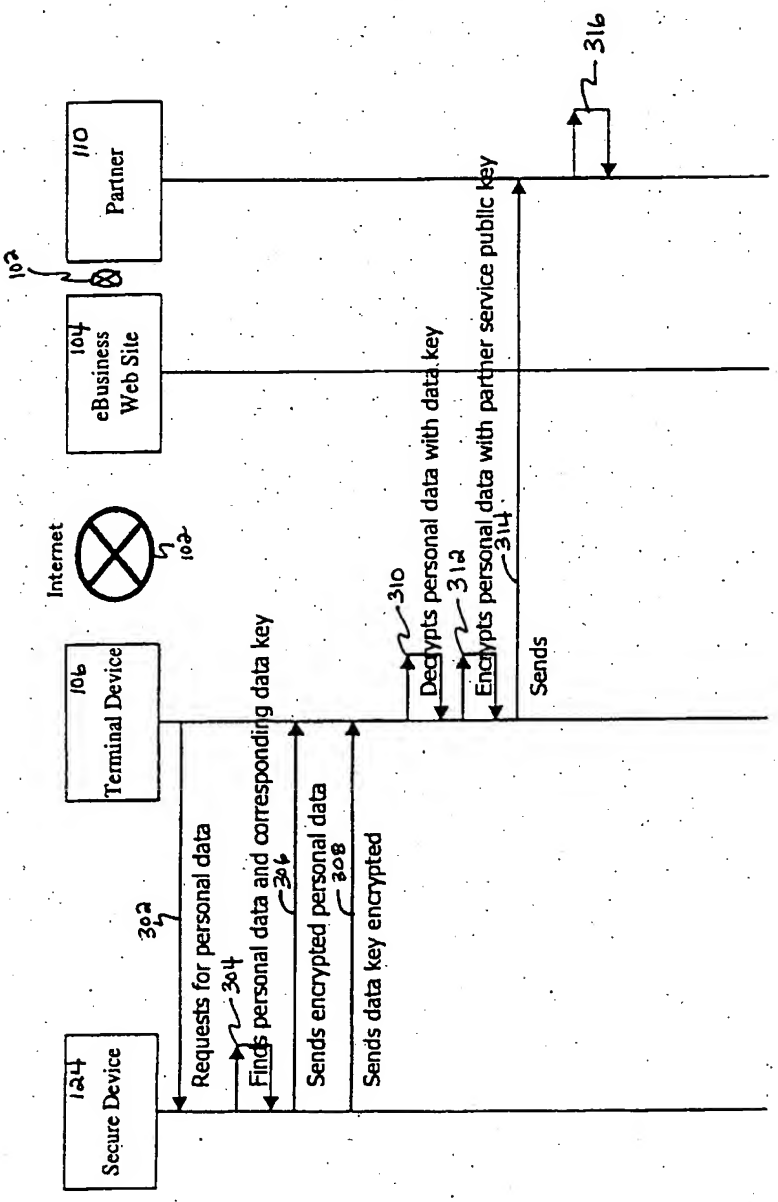
110
Partner
316
102
104
eBusiness Web Site
Internet
108
106
Terminal Device
310
Decrypts personal data with data key
312
Encrypts personal data with partner service public key
314
Sends
302
Requests for personal data
304
Finds personal data and corresponding data key
306
Sends encrypted personal data
308
Sends data key encrypted
124
Secure Device

FIG. 3

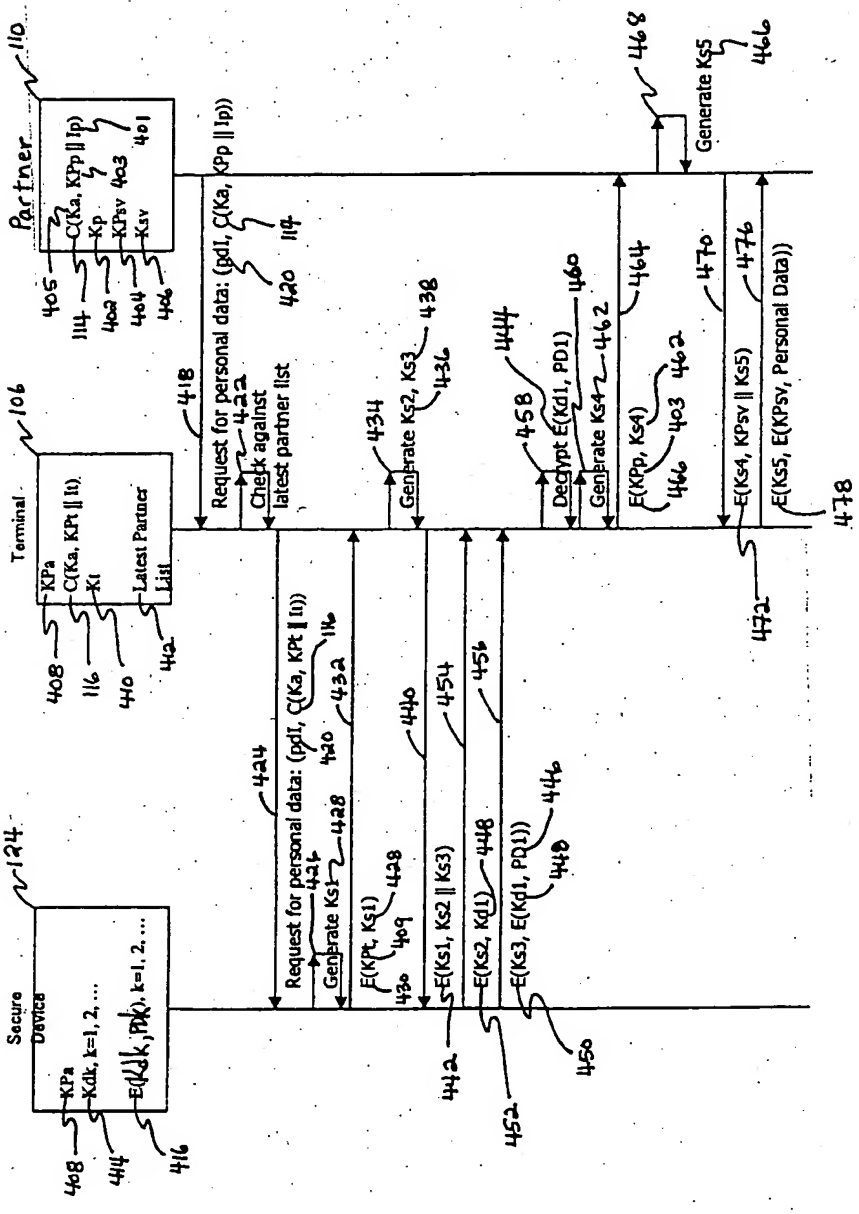
Partner
110
C(Ka, KPp || Ip)
Kp
KPsv
Ksv
401
405
114
402
403
404
406
Request for personal data: (pdl, C(Ka, KPp || Ip))
420
114
418
Terminal
106
KPa
C(Ka, KPt || It)
Kt
Latest Partner List
408
116
410
412
Check against latest partner list
422
Generate Ks2, Ks3
434
436
438
Request for personal data: (pdl, C(Ka, KPt || It))
424
420
116
432
Secure Device
124
KPa
Kdk, k=1, 2, ...
E(Kdk, PIK), k=1, 2, ...
408
414
416
Generate Ks1
426
428
E(KPt, Ks1)
429
430
E(Ks1, Ks2 || Ks3)
440
454
E(Ks2, Kd1)
448
456
E(Ks3, E(Kd1, PD1))
446
450
452
Decrypt E(Kd1, PD1)
444
458
460
Generate Ks4
462
E(KPp, Ks4)
464
466
403
462
Generate Ks5
468
466
E(Ks4, KPsv || Ks5)
470
476
E(Ks5, E(KPsv, Personal Data))
472
478

FIG. 4

500

Name (502)	Expression (504)	Description (506)
Encryption (509)	E(K, D)	The result of encrypting information "D" with key "K"
Hash (510)	H(D)	The result of hashing information "D"
Concatenation	A ‖ B	Concatenation of "A" and "B"
CA Private Key (405)	Ka	A private key used by a CA to sign certificate
CA Public Key (408)	KPa	A public key corresponding to Ka
Partner Information (401)	Ip	The information pertaining to the partner
Partner Private Key (402)	Kp	A private key owned by the partner
Partner Public Key (403)	KPp	A public key corresponding to Kp
Partner Certificate (114)	C(Ka, KPp ‖ Ip)	X.509 certificate for the partner
Partner Service Private Key (406)	Ksv	A private key owned by the partner service
Partner Service Public Key (404)	KPsv	A public key corresponding to Ksv
Terminal Information (407)	It	The information pertaining to the partner
Terminal Private Key (410)	Kt	A private key owned by the terminal
Terminal Public Key (409)	KPt	A public key corresponding to Kt
Terminal Certificate (116)	C(Ka, KPt ‖ It)	X.509 certificate for the terminal
Personal Data	PDk, k=1,2,...	Personal data for eBusiness service transaction
Personal Data Encryption Key (408)	Kdk, k=1, 2, ...	A symmetric key to encrypt personal data (stored in the TRM of the PIN-SMMC)
Encrypted Personal Data (416)	E(PDk, Kdk), k=1, 2, ...	Personal data stored in an encrypted format in the flash memory portion of the PIN-SMMC
Personal Data information (420)	pdI	Information related to identifying the appropriate personal data to submit to the partner site
Session Key (512)	Ksk, k=1, 2, ...	A symmetric key generated in real-time to encrypt a communication session

FIG. 5

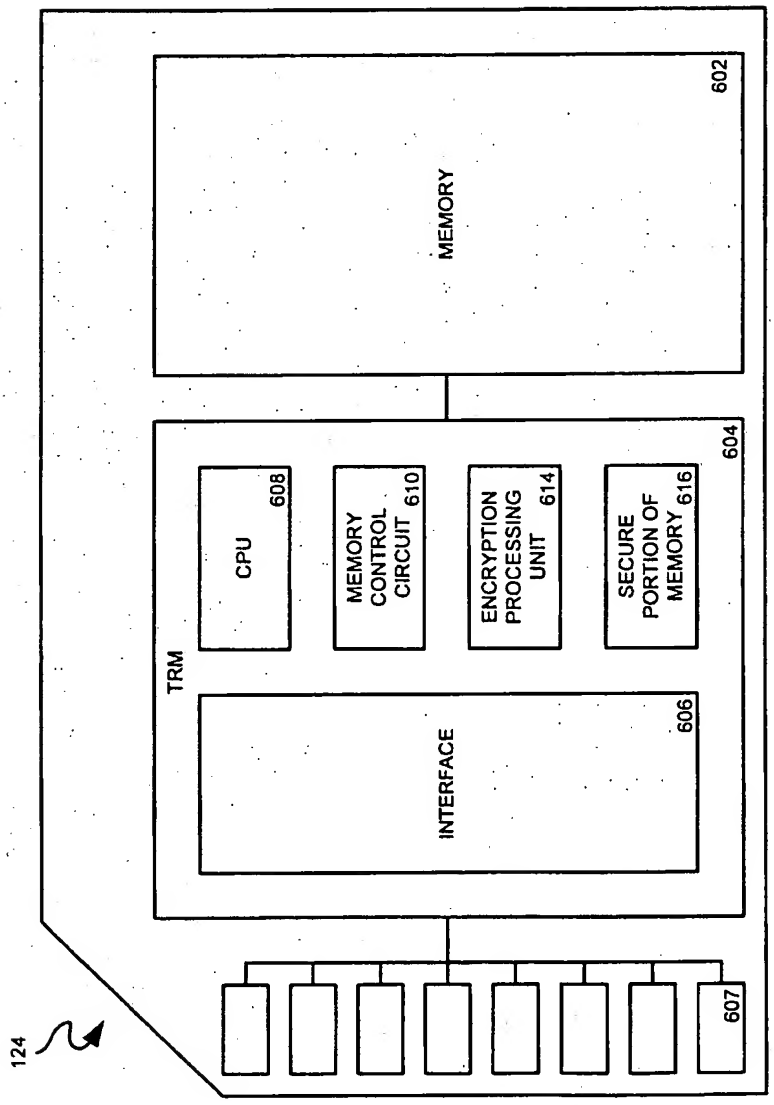
602
MEMORY
604
TRM
CPU
608
MEMORY CONTROL CIRCUIT
610
ENCRYPTION PROCESSING UNIT
614
SECURE PORTION OF MEMORY
616
606
INTERFACE
607
124

FIG. 6

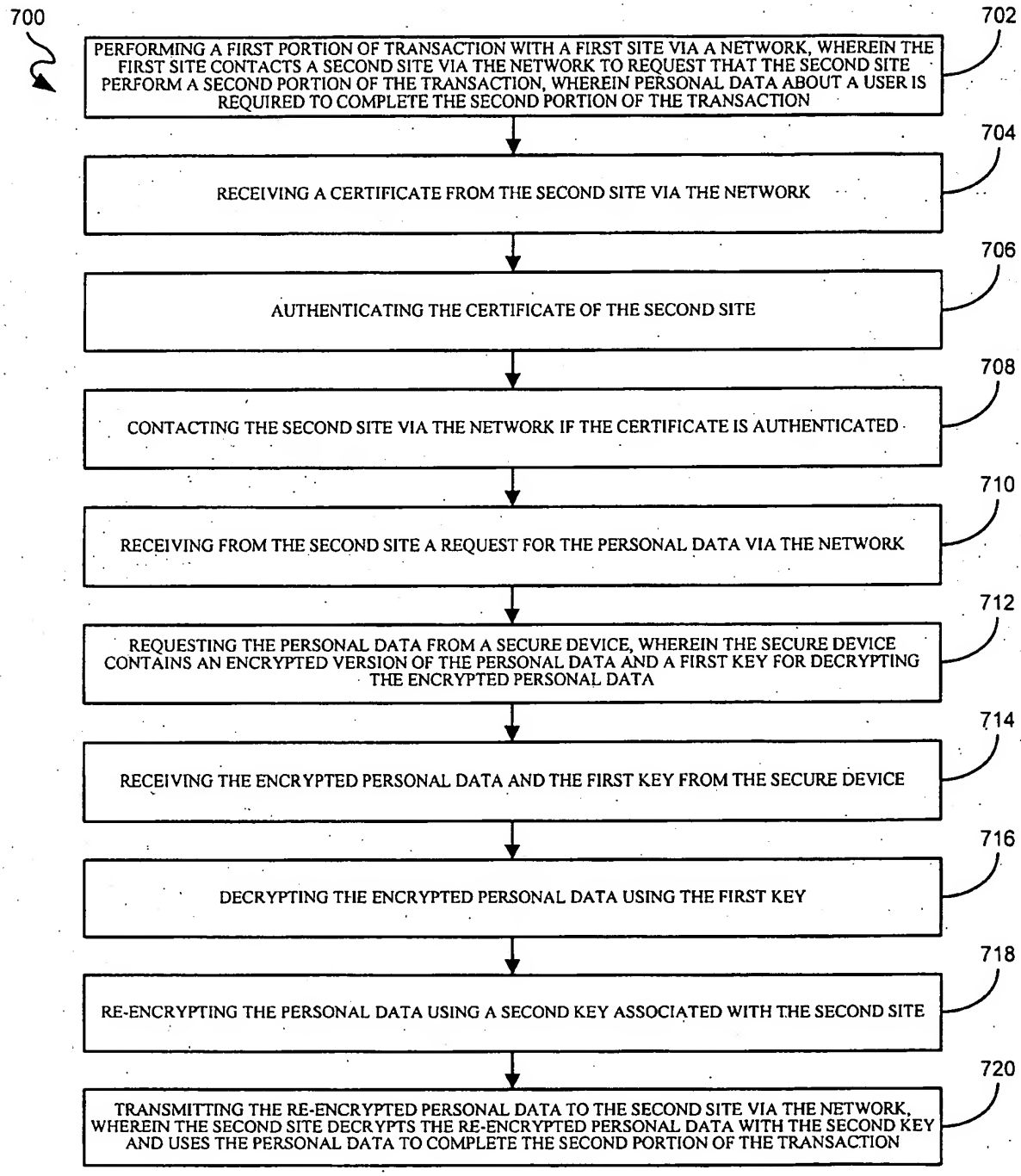
700
PERFORMING A FIRST PORTION OF TRANSACTION WITH A FIRST SITE VIA A NETWORK, WHEREIN THE FIRST SITE CONTACTS A SECOND SITE VIA THE NETWORK TO REQUEST THAT THE SECOND SITE PERFORM A SECOND PORTION OF THE TRANSACTION, WHEREIN PERSONAL DATA ABOUT A USER IS REQUIRED TO COMPLETE THE SECOND PORTION OF THE TRANSACTION
702
RECEIVING A CERTIFICATE FROM THE SECOND SITE VIA THE NETWORK
704
AUTHENTICATING THE CERTIFICATE OF THE SECOND SITE
706
CONTACTING THE SECOND SITE VIA THE NETWORK IF THE CERTIFICATE IS AUTHENTICATED
708
RECEIVING FROM THE SECOND SITE A REQUEST FOR THE PERSONAL DATA VIA THE NETWORK
710
REQUESTING THE PERSONAL DATA FROM A SECURE DEVICE, WHEREIN THE SECURE DEVICE CONTAINS AN ENCRYPTED VERSION OF THE PERSONAL DATA AND A FIRST KEY FOR DECRYPTING THE ENCRYPTED PERSONAL DATA
712
RECEIVING THE ENCRYPTED PERSONAL DATA AND THE FIRST KEY FROM THE SECURE DEVICE
714
DECRYPTING THE ENCRYPTED PERSONAL DATA USING THE FIRST KEY
716
RE-ENCRYPTING THE PERSONAL DATA USING A SECOND KEY ASSOCIATED WITH THE SECOND SITE
718
TRANSMITTING THE RE-ENCRYPTED PERSONAL DATA TO THE SECOND SITE VIA THE NETWORK, WHEREIN THE SECOND SITE DECRYPTS THE RE-ENCRYPTED PERSONAL DATA WITH THE SECOND KEY AND USES THE PERSONAL DATA TO COMPLETE THE SECOND PORTION OF THE TRANSACTION
720

FIG. 7

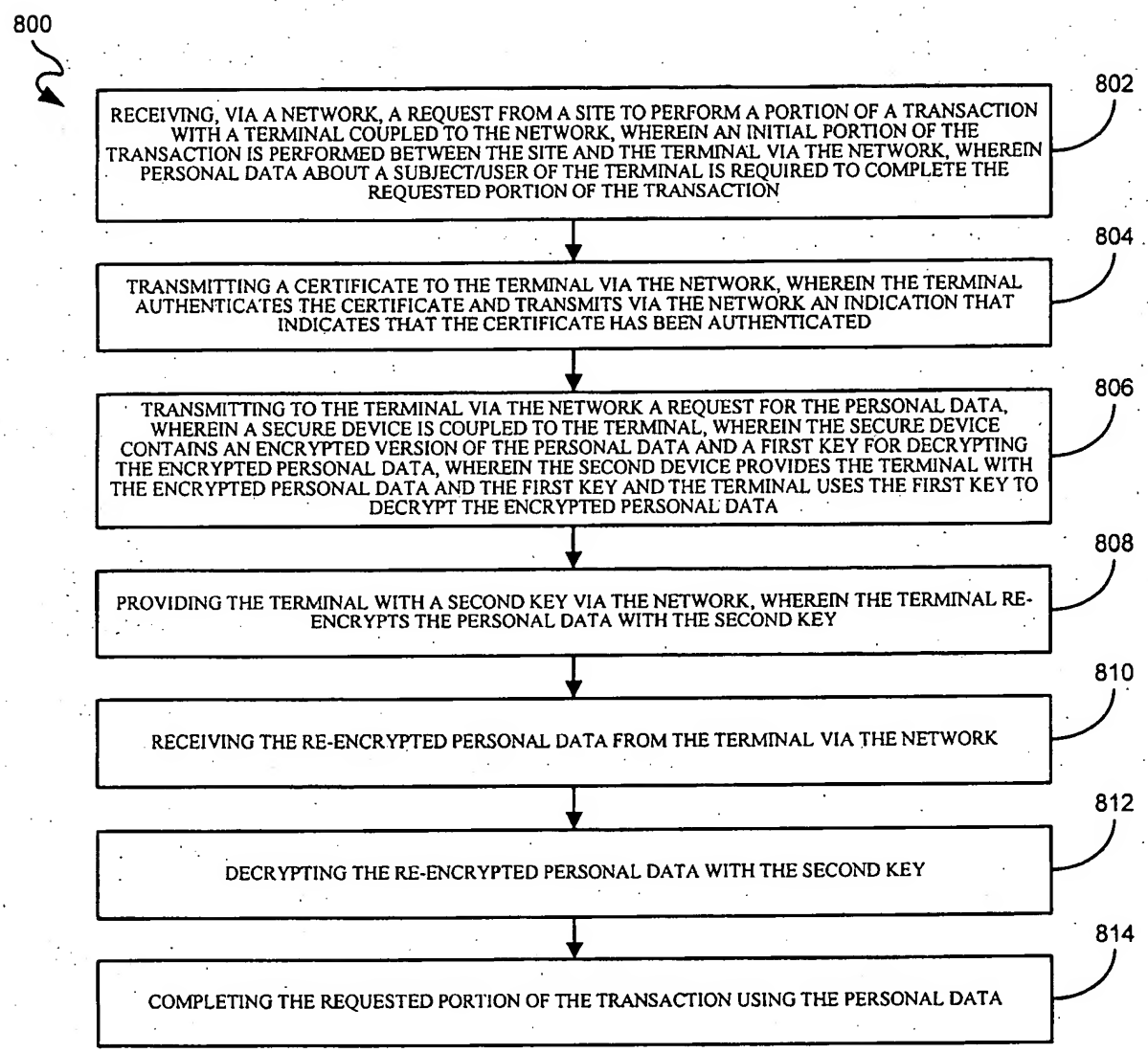
800
RECEIVING, VIA A NETWORK, A REQUEST FROM A SITE TO PERFORM A PORTION OF A TRANSACTION WITH A TERMINAL COUPLED TO THE NETWORK, WHEREIN AN INITIAL PORTION OF THE TRANSACTION IS PERFORMED BETWEEN THE SITE AND THE TERMINAL VIA THE NETWORK, WHEREIN PERSONAL DATA ABOUT A SUBJECT/USER OF THE TERMINAL IS REQUIRED TO COMPLETE THE REQUESTED PORTION OF THE TRANSACTION
802
TRANSMITTING A CERTIFICATE TO THE TERMINAL VIA THE NETWORK, WHEREIN THE TERMINAL AUTHENTICATES THE CERTIFICATE AND TRANSMITS VIA THE NETWORK AN INDICATION THAT INDICATES THAT THE CERTIFICATE HAS BEEN AUTHENTICATED
804
TRANSMITTING TO THE TERMINAL VIA THE NETWORK A REQUEST FOR THE PERSONAL DATA, WHEREIN A SECURE DEVICE IS COUPLED TO THE TERMINAL, WHEREIN THE SECURE DEVICE CONTAINS AN ENCRYPTED VERSION OF THE PERSONAL DATA AND A FIRST KEY FOR DECRYPTING THE ENCRYPTED PERSONAL DATA, WHEREIN THE SECOND DEVICE PROVIDES THE TERMINAL WITH THE ENCRYPTED PERSONAL DATA AND THE FIRST KEY AND THE TERMINAL USES THE FIRST KEY TO DECRYPT THE ENCRYPTED PERSONAL DATA
806
PROVIDING THE TERMINAL WITH A SECOND KEY VIA THE NETWORK, WHEREIN THE TERMINAL RE-ENCRYPTS THE PERSONAL DATA WITH THE SECOND KEY
808
RECEIVING THE RE-ENCRYPTED PERSONAL DATA FROM THE TERMINAL VIA THE NETWORK
810
DECRYPTING THE RE-ENCRYPTED PERSONAL DATA WITH THE SECOND KEY
812
COMPLETING THE REQUESTED PORTION OF THE TRANSACTION USING THE PERSONAL DATA
814

FIG. 8

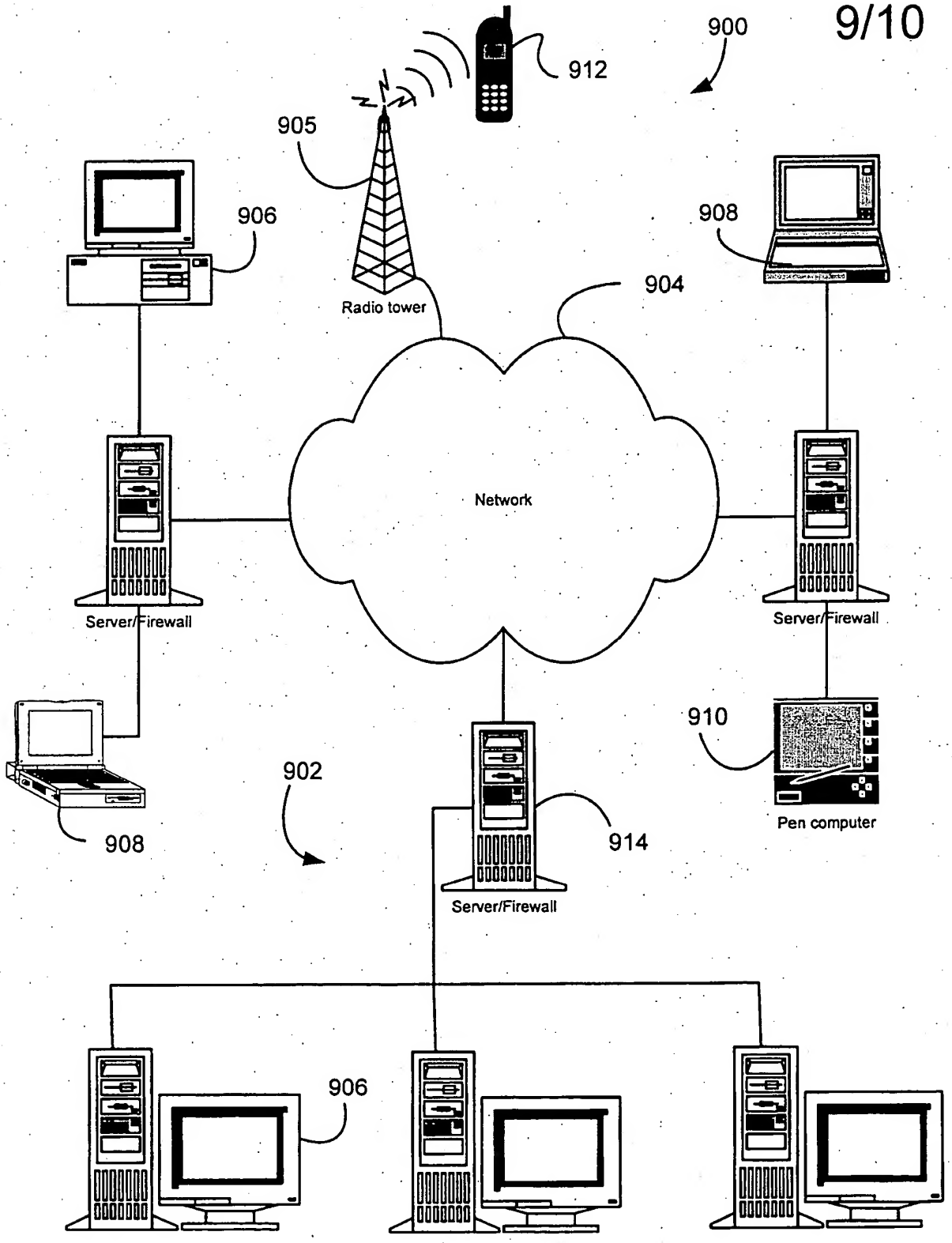
900
912
905
906
908
Radio tower
904
Network
Server/Firewall
Server/Firewall
910
Pen computer
902
908
914
Server/Firewall
906

FIG. 9

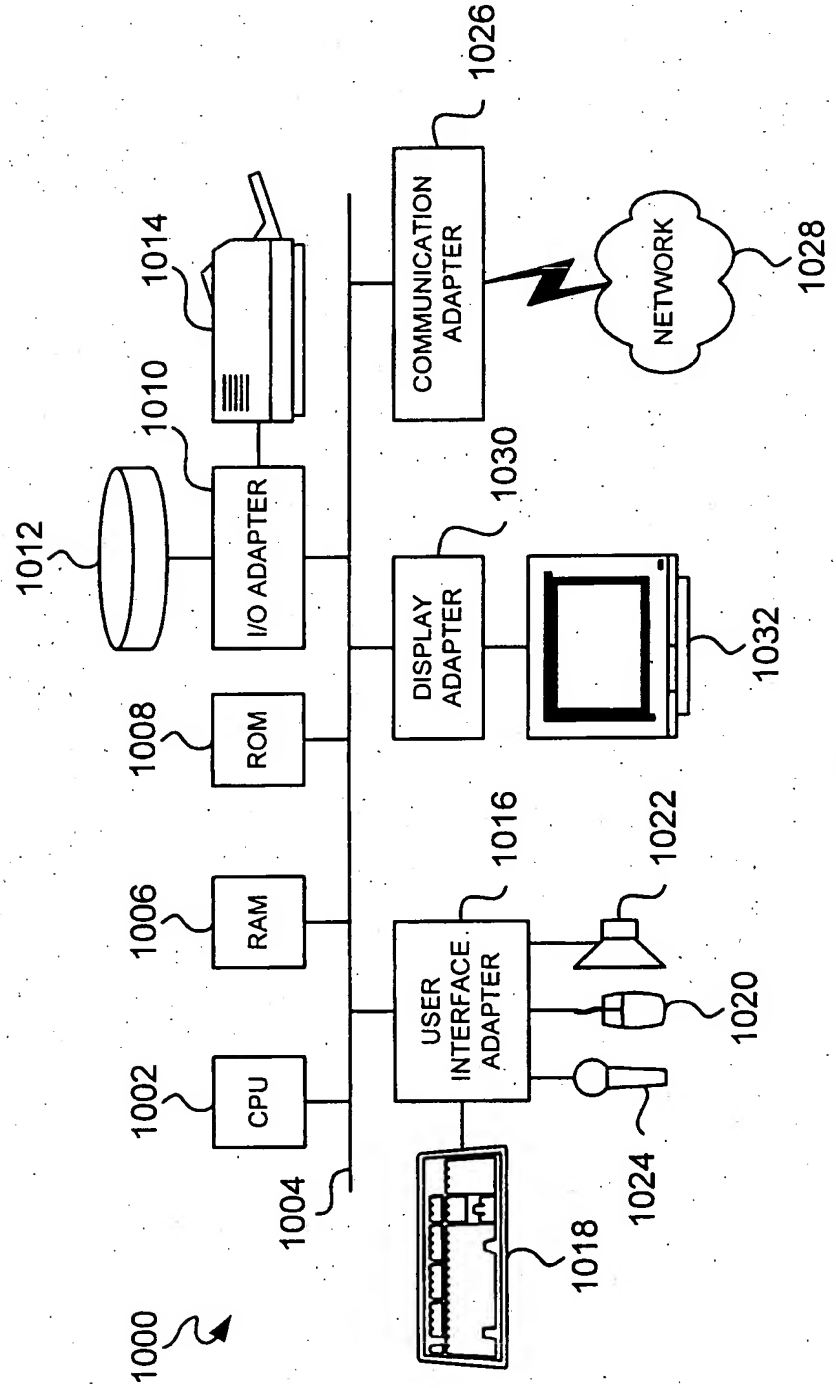
1000
1002
CPU
1004
1006
RAM
1008
ROM
1010
I/O ADAPTER
1012
1014
1016
USER INTERFACE ADAPTER
1018
1020
1022
1024
1026
COMMUNICATION ADAPTER
1028
NETWORK
1030
DISPLAY ADAPTER
1032

FIG. 10